UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,144	02/17/2004	Aaron Sauve	14917.1241US01/307917.01	2246

27488 7590 09/14/2010

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
09/14/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,144	SAUVE ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26,28,29,31,33,36-56 and 58-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26,28,29,31,33,36-56 and 58-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on 1/22/10.

2. Claims 1-26, 28, 29, 31, 33, 36-56 and 58-66 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/22/10 has been entered.

Definitions and Significant Terms

4. The following portion of Applicant's specification was deemed pertinent for the limitation "[a]ccording ... a trust level of a plurality of trust level security settings of the browser to the object" (see claim 1): paragraphs [0023-0066] on pgs. 5-18. In particular, paragraph [0025] discloses a Trust analyzer 210 assessing a level of trust to a detected object based on the content, source or action associated with the object 208; paragraph [0033] discloses that the level of trust my be considered to be tiered ("That is, more than being determined to be merely trusted or untrusted, object 208 may be accorded a variable level of trust in accordance with the content, source, and action

corresponding to object 208."); and paragraphs [0038-0066] disclose further details of the trust level analysis process.

5. "computer-readable storage medium" (see claim 21): in view of pgs. 26-27 of Applicant's specification, this limitation is interpreted to be directed to only statutory inventions under 35 USC 101, i.e. it does not include within its scope, under the broadest reasonable interpretation, signal inventions. Paragraph [0092] identifies that computer readable media may comprise "computer storage media" and "communications media." Furthermore, paragraphs [0093-0094] classify "computer storage media" as directed to hardware-related storage devices, whereas "communications media" are directed to transitory propagation signals. Hence, a "computer-readable storage medium" is directed to hardware-related storage devices including volatile and non-volatile memory.

Response to Arguments

6. Applicant's arguments with respect to the amended claims are moot in view of the new rejections.

Claim Objections

7. Claims 5, 9, 13, 16, 63 and 66 are objected to because of the following informalities:

8. Claims 5, 9, 13 and 16 recite "[a] method according to Claim 1, wherein according the one or more of the plurality trust level security settings of the browser to

the object evaluates criteria including ..."; however, claim 1 has been amended to recite "according ... a trust level of the plurality trust level security settings of the browser to the object." In claims 5, 9, 13 and 16, replace "one or more" with "a trust level."

9. Claims 63 and 66 recite "[a]n apparatus according to Claim 56, wherein the means for performing the trust analysis evaluates criteria including ..."; however, claim 56 has been amended to recite "wherein the means for performing the trust analysis for the object evaluates a trust level according to the object." In claims 63 and 66, replace "criteria" with "a trust level accorded to the object."

Claim Rejections - 35 USC § 102

10. Claims 1, 3, 4, 9, 10, 16, 17, 20, 36, 38-41, 44, 45, 51, 52, 55, 56, 58, 60-63, 65 and 66 are rejected under 35 U.S.C. 102(b) as being anticipated by Jerger et al. US 6,321,334 (hereinafter Jerger).

11. As per claim 1, Jerger discloses a tiered security system and method for managing active content downloaded from a network on to a browser. The invention implements a tiered system where each lower tier provides a more fine grained definition of system policy. This invention classifies network content by designating general security zones, which encompass Web sites and related collection of pages, as well as distinguishing different types of active content downloaded from these sites. Security level designations are accorded on both a coarse grain level (security zones)

and a fine grained level (active content within a downloaded page). Fig. 2 illustrates the architecture of the security system, which is reprinted below.

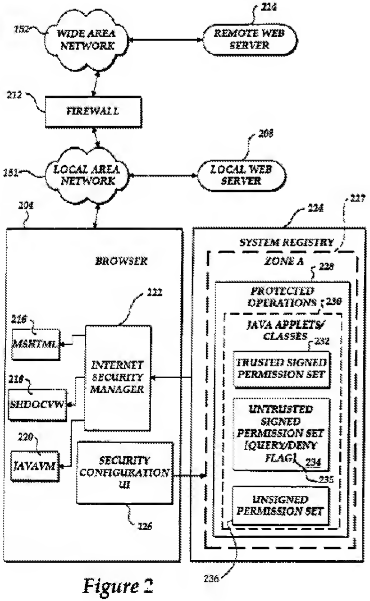

Figure 2

Fig. 5A illustrates a dialog window to configure security levels for Java applications that are downloaded from the network, which is reprinted below.

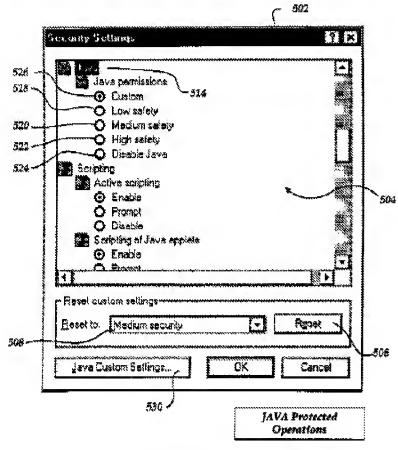

Figure 5A

12. Each of the security level settings defines a preconfigured permission set for the active content. See generally, col. 20, line 43-col. 28, line 34, "Administering Permissions in Zones."

13. Hence, Jerger discloses a method of displaying a web page by a browser at a client device, comprising:

a. detecting, by the browser at the client device, an object associated with a web page, wherein the object is an activatable object (col. 11, lines 11-26; col.

13, lines 5-10, the security model is incorporated into a web browser; col. 14, lines 12-44);

b. according, by the browser at the client device, as part of displaying the web page, a trust level of a plurality of trust level security settings of the browser to the object, wherein the according comprises evaluating a content, source, or action of the object (see col. 3, lines 19-26, "prior to performing a protected operation, the mechanism of the invention determines the action to perform, based on the current Web site's security zone, the requested operation, and the security setting corresponding to the requested operation, and the security setting corresponding to the requested operation and the Web site's zone"; col. 21, lines 15-20, a user can specify low safety, medium safety and high safety with respect to JAVA permissions; col. 22, lines 11-col. 25, line 60, each safety setting defines a set of operations and privileges accorded to an activatable object [see col. 22, line 50-col. 23, line 28]; these operations and privileges are further dependent on whether the content is trusted or not trusted; hence, whether or not an object exceeds the designated level of trust depends on various characteristics of the object);

c. suppressing the object when the trust level accorded to the object does not reach a threshold trust level based on variable combinations of the content, source, and action of the object (col. 31, line 46-col. 33, line 22; see figs. 13A-C).

14. As per claim 3, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger. In addition, the object is embedded in the web page, and includes any one of downloadable code, a link to a URL, a popup window, graphic data, a video file, an audio file, and a text file. See Jerger, col. 10, lines 31-43, the object list an applet.

15. As per claim 4, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger. In addition, the object is a link to an object on a remote server, wherein further the object on the remote server includes any one of downloadable code, a URL, a popup window, graphic data, a video file, an audio file, and a text file. See Jerger, col. 10, lines 31-43, the object list a link pointing to an applet stored on a server.

16. As per claims 9 and 10, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger. In addition, Jerger discloses wherein according the one or more of the plurality of trust level security settings of the browser to the object evaluates criteria including whether the object is to be rendered and whether a download flag is set, and wherein further suppressing the object includes displaying a prompt to indicate the suppression of the object based upon a positive evaluation of any of the criteria; wherein the prompt is a modal prompt to provide a user with an activation choice (col. 19, line 22-col. 20, line 12, settings for protected operations include enabling/disabling/prompting scripting of Java applets and Java Permission, and scripting, download and running of ActiveX; col. 20, lines 22-34, a security warning

dialog window informs the user of the operation to be performed; the user can select whether or not the operation is performed; col. 22, line 50-col. 23, line 49).

17. As per claims 16, 17 and 20, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger. In addition, Jerger discloses further discloses wherein according the one or more of the plurality of trust level security settings of the browser to the object evaluates criteria including whether the object is beneath a security setting and whether a security setting flag is set, and wherein further suppressing the object includes displaying a prompt to indicate the suppression of the object based upon a positive evaluation of any of the criteria; wherein the prompt is a modal prompt to provide a user with an activation choice; wherein suppressing the object includes displaying a user interface to describe the content of the suppressed object and to provide a user with an opportunity to activate the content of the suppressed object (see col. 21, lines 15-20, a user can specify low safety, medium safety and high safety with respect to JAVA permissions; col. 22, lines 11-col. 25, line 60, each safety setting defines a set of operations and privileges accorded to an activatable object [see col. 22, line 50-col. 23, line 28], these operations and privileges are further dependent on the whether the content is trusted or not trusted; col. 20, lines 22-34, a security warning dialog window informs the user of the operation to be performed and the web site that is requesting the operation; the user can select whether or not the operation is performed).

18. As per claims 36, 38-41, 44, 45, 51, 52 and 55, they are apparatus claims corresponding to claims 1, 3, 4, 9, 10, 16, 17 and 20, and they do not teach or define above the information claimed in claims 1, 3, 4, 9, 10, 16, 17 and 20. Therefore, claims 36, 38-41, 44, 45, 51, 52 and 55 are rejected as being anticipated by Jerger for the same reasons set forth in the rejections of claims 1, 3, 4, 9, 10, 16, 17 and 20.

19. As per claims 56, 58, 60-63, 65 and 66, they are apparatus claims corresponding to claims 1, 3, 4, 9, 10, 16, 17, 20, 36-41, 44, 45, 51, 52 and 55, and they do not teach or define above the information claimed in claims 1, 3, 4, 9, 10, 16, 17, 20, 36-41, 44, 45, 51, 52 and 55. Therefore, claims 56, 58, 60-63, 65 and 66 are rejected as being anticipated by Jerger for the same reasons set forth in the rejections of claims 1, 3, 4, 9, 10, 16, 17, 20, 36-41, 44, 45, 51, 52 and 55.

Claim Rejections - 35 USC § 103

20. Claims 2, 37 and 59 are rejected under 35 USC 103(a) as being unpatentable over Jerger in view of Touboul US 6,092,194 (hereinafter Touboul '194).

21. As per claim 2, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger is incorporated herein. Although Jerger discloses according the trust levels to other types of active content besides JAVA executables (see col. 22, lines 4-11), Jerger does not expressly disclose the object is one of a COM object or an ActiveX control. Touboul '194 discloses a system and method for protecting a computer from hostile

downloadables, including Java applets, ActiveX control, JavaScript script or Visual Basic script. See col. 1, lines 65-67; col. 2, lines 21-37; col. 9, lines 63-65. This invention performs several tests on a downloadable, including whether an administrator has designated an override to allow or deny this particular downloadable, whether the downloadable performs potentially hostile operations, whether the downloadable was signed by a certificate authority, and whether the downloadable comes from a trusted source. See col. 5, line 17-col. 6, line 48. The results of these tests are then forwarded to a logical engine; the logical engine examines the results of the tests and a security policy to determine whether to allow or block the Downloadable. See col. 6, lines 49-67. Hence, in view of the invention of Touboul '194, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Jerger such that the object is one of a COM object or an ActiveX control. One would be motivated to do to provide a fine grained definition of security policy on any type of active content that is downloaded from the network. The aforementioned cover the limitations of claim 2.

22. As per claims 37 and 59, they are claims corresponding to claims 2, 36 and 56, and they do not teach or define above the information claimed in claims 2, 36 and 56. Therefore, claims 37 and 59 are rejected as being unpatentable over Jerger in view of Touboul '194 for the same reasons set forth in the rejections of claims 2, 36 and 56.

23. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerger in view of Donohue USPN 6,202,207 (hereinafter Donohue).

24. As per claims 5 and 6, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger. In addition, Jerger discloses wherein according the one or more of the plurality of trust level security settings of the browser to the object evaluates criteria including whether the object is from a trusted source and whether a download flag is set, and wherein further suppressing the object includes displaying a prompt to indicate the suppression of the object based upon a positive evaluation of any of the criteria; wherein the prompt is a modal prompt to provide a user with an activation choice (col. 19, line 22-col. 20, line 12, settings for protected operations include enabling/disabling/prompting scripting of Java applets and Java Permission, and scripting, download and running of ActiveX; col. 20, lines 22-34, a security warning dialog window informs the user of the operation to be performed; the user can select whether or not the operation is performed; col. 22, line 50-col. 23, line 49, permission configuration options are determined based on whether the object is signed or unsigned content). However, Jerger does not disclose the criteria includes whether the object is to upgrade an existing object. Donohue discloses a method for updating software, including accessing a web site to download resources to update versions of a software, downloading the resources, verifying the resources and building the updated version, wherein verification step includes verifying the signature of the downloaded resource, verifying allowable growth paths from the current to the updated versions based on

license restrictions, and verifying other authentication information including password and/or a database usage parameter value. Col. 10:16-12:48. It would be obvious to one of ordinary skill in the art at the time the invention was made for the criteria to include whether the object is to upgrade an existing object, since this ensures that only trusted resources are used to upgrade an existing object. Donohue, 10:50-58. The aforementioned cover the limitations of claims 5 and 6.

25. Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerger in view of Donohue, and further in view of Pennell et al. US Patent Application Publication No. 20030098883. (hereinafter Pennell)

26. As per claim 8, the rejection of claim 5 under 35 USC 103(a) as being unpatentable over Jerger in view of Donohue is incorporated herein. Neither Jerger nor Donohue disclose wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. Pennell discloses a method for blocking "bad" windows and displaying "good" windows, wherein a window analyzer identifies whether a window is "good" or "bad" based on a list having characteristics of the window, including the source of the window (paragraph 0043), and wherein when a "bad" window is identified, blocking the window and displaying a prompt to indicate the suppression of the window based on this identification. (paragraph 0081) Pennell further discloses the prompt is a modeless prompt to advise a user of the object being suppressed and provides the user with a

subsequent activation choice. (Pennell, paragraph 0081, 5th, 6th sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for the step of suppressing the object to include displaying a prompt to indicate the suppression of the object based upon the positive evaluation of any of the criteria; wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. One would be motivated to do so for a user-friendly manner of informing the user of a preventive measure by the invention. The aforementioned cover the limitations of claim 8.

27. As per claim 7, the rejection of claim 8 under 35 USC 103(a) as being unpatentable over Jerger in view of Donohue and Pennell is incorporated herein. Furthermore, it is notoriously well known in the art to provide a description of an action to the user with a modeless prompt. Examples abound: modeless prompts describing status and actions have been a part of GUI-based OS systems from their inception. The basic rational for providing a description with a modeless prompt is that it informs the user 1) an action was taken and 2) what the action was. Furthermore, a modeless prompt that is displayed when an object is suppressed without any description of the object being suppressed is analogous to an alert of a situation without any description of the situation; in both scenarios, a message that identified what has occurred enables the receiver of the prompt or alert to properly react to the prompt or alert. Official Notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made for the modeless prompt to provide a description of the object

being suppressed. One would be motivated to do so to provide the user with a more user-friendly experience as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 7.

28. Claims 11-15, 18, 19, 21, 23-26, 28, 29, 31, 33, 42, 43, 46-50, 53, 54 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerger in view of Pennell

29. As per claims 11 and 12, the rejection of claim 9 under 35 USC 102(b) as being anticipated by Jerger is incorporated herein. Moreover, Jerger does not disclose wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. Pennell discloses a method for blocking "bad" windows and displaying "good" windows, wherein a window analyzer identifies whether a window is "good" or "bad" based on a list having characteristics of the window, including the source of the window (paragraph 0043), and wherein when a "bad" window is identified, blocking the window and displaying a prompt to indicate the suppression of the window based on this identification. (paragraph 0081) Pennell further discloses the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. (Pennell, paragraph 0081, 5th, 6th sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for the step of suppressing the object to include displaying a prompt to indicate the suppression of the object based upon the positive evaluation of any of the criteria; wherein the prompt is a modeless prompt to advise a

user of the object being suppressed and to provide the user with a subsequent activation choice. One would be motivated to do so for a user-friendly manner of informing the user of a preventive measure by the invention. The aforementioned cover the limitations of claims 11 and 12.

30. As per claim 13, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Jerger is incorporated herein. Jerger does not disclose the step of according the one or more of the plurality of trust level security settings of the browser to the object is based on whether the object is a popup window, and the step of suppressing the object includes displaying a prompt to indicate the suppression of the object based upon a positive determination. Pennell discloses it is desirous to block certain popup windows to prevent annoyances to a user browsing experience and discloses a method for blocking "bad" popup windows and displaying "good" popup windows, wherein a window analyzer identifies whether a window is "good" or "bad" based on a list having characteristics of the window, including the source of the window (paragraphs 0006-0008 and 0043), and wherein when a "bad" window is identified, blocking the window and displaying a prompt to indicate the suppression of the window based upon a positive determination. (paragraph 0081) It would be obvious to one of ordinary skill in the art at the time the invention was made for the step of according the one or more of the plurality of trust level security settings of the browser to the object is based on whether the object is a popup window, and the step of suppressing the object includes displaying a prompt to indicate the suppression of the object based upon a

positive determination. One would be motivated to do so to block unwanted popups from cluttering the screen and for generating a user-friendly manner of informing the user of a preventive measure by the invention. The aforementioned cover the limitations of claim 13.

31. As per claim 14, the rejection of claim 13 under 35 USC 103(a) as being unpatentable over Jerger in view of Pennell is incorporated herein. In addition, the prompt is a modeless prompt to advise a user of the object being suppressed. (Pennell, paragraph 0081, 5th sentence)

32. As per claim 15, the rejection of claim 13 under 35 USC 103(a) as being unpatentable over Jerger in view of Pennell is incorporated herein. In addition, the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with an activation choice. (Pennell, paragraph 0081, 5th and 6th sentence)

33. As per claims 18 and 19, the rejection of claim 16 under 35 USC 102(b) as being anticipated by Jerger is incorporated herein. Moreover, Jerger does not disclose wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. Pennell discloses a method for blocking "bad" windows and displaying "good" windows, wherein a window analyzer identifies whether a window is "good" or "bad" based on a list having

characteristics of the window, including the source of the window (paragraph 0043), and wherein when a "bad" window is identified, blocking the window and displaying a prompt to indicate the suppression of the window based on this identification. (paragraph 0081) Pennell further discloses the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. (Pennell, paragraph 0081, 5th, 6th sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for the step of suppressing the object to include displaying a prompt to indicate the suppression of the object based upon the positive evaluation of any of the criteria; wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. One would be motivated to do so for a user-friendly manner of informing the user of a preventive measure by the invention. The aforementioned cover the limitations of claims 18 and 19.

34. As per claims 21, 23-26, 28, 29, 31 and 33, the rejections of claims 1, 3, 4, 9, 10, 16, 17 and 20 under 35 USC 102(b) as being anticipated by Jerger are incorporated herein. Jerger further discloses a computer-readable storage medium having one or more instructions that, when read, cause one or more processors on a client device to execute steps as recited in claims 1-4. See col. 13, lines 5-10, the security model is incorporated into a web browser. Jerger does not disclose wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice; wherein the one or more instructions to

determine the trust level security setting for the object causes the one or more processors to determine whether the object is a popup window, and wherein further the one or more instructions to provide an activation opportunity for the action causes the one or more processors to display a user interface indicating the suppression of the action due to a positive determination and offering an activation option. Pennell discloses a method for blocking "bad" windows and displaying "good" windows, wherein a window analyzer identifies whether a window is "good" or "bad" based on a list having characteristics of the window, including the source of the window (paragraph 0043), and wherein when a "bad" window is identified, blocking the window and displaying a prompt to indicate the suppression of the window based on this identification. (paragraph 0081) Pennell further discloses the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice. (Pennell, paragraph 0081, 5th, 6th sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for the step of suppressing the object to include displaying a prompt to indicate the suppression of the object based upon the positive evaluation of any of the criteria; wherein the prompt is a modeless prompt to advise a user of the object being suppressed and to provide the user with a subsequent activation choice; wherein the one or more instructions to determine the trust level security setting for the object causes the one or more processors to determine whether the object is a popup window, and wherein further the one or more instructions to provide an activation opportunity for the action causes the one or more processors to display a user interface indicating the suppression of the action due to a positive

determination and offering an activation option. One would be motivated to do so for a user-friendly manner of informing the user of a preventive measure by the invention.

35. Furthermore, it is notoriously well known in the art to provide a description of an action to the user with a modeless prompt. Examples abound: modeless prompts describing status and actions have been a part of GUI-based OS systems from their inception. The basic rational for providing a description with a modeless prompt is that it informs the user 1) an action was taken and 2) what the action was. Furthermore, a modeless prompt that is displayed when an object is suppressed without any description of the object being suppressed is analogous to an alert of a situation without any description of the situation; in both scenarios, a message that identified what has occurred enables the receiver of the prompt or alert to properly react to the prompt or alert. Official Notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made for the modeless prompt to provide a description of the object being suppressed. One would be motivated to do so to provide the user with a more user-friendly experience as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 21, 23-26, 28, 29, 31 and 33.

36. As per claims 42, 43, 46-50, 53 and 54, they are apparatus claims corresponding to claims 11-15, 18, 19, 21-26, 28, 29, 31 and 33, and they do not teach or define above the information claimed in claims 11-15, 18, 19, 21-26, 28, 29 and 33. Therefore, claims 42, 43, 46-50, 53 and 54 are rejected as being unpatentable over Jerger in view

of Pennell for the same reasons set forth in the rejections of claims 11-15, 18, 19, 21-26, 28, 29, 31 and 33.

37. As per claim 64, it is an apparatus claim corresponding to claims 31 and 56, and it does not teach or define above the information claimed in claims 31 and 56. Therefore, claim 64 is rejected as being unpatentable over Jerger in view of Pennell for the same reasons set forth in the rejections of claims 31 and 56.

38. Claim 22 is rejected under 35 USC 103(a) as being unpatentable over Jerger in view of Pennell, and further in view of Touboul.

39. As per claim 22, the rejection of claim 21 under 35 USC 103(a) as being unpatentable over Jerger in view of Pennell is incorporated herein. Although Jerger discloses according the trust levels to other types of active content besides JAVA executables (see col. 22, lines 4-11), Jerger does not expressly disclose the object is one of a COM object or an ActiveX control. Touboul '194 discloses a system and method for protecting a computer from hostile downloadables, including Java applets, ActiveX control, JavaScript script or Visual Basic script. See col. 1, lines 65-67; col. 2, lines 21-37; col. 9, lines 63-65. This invention performs several tests on a downloadable, including whether an administrator has designated an override to allow or deny this particular downloadable, whether the downloadable performs potentially hostile operations, whether the downloadable was signed by a certificate authority, and

whether the downloadable comes from a trusted source. See col. 5, line 17-col. 6, line 48. The results of these tests are then forwarded to a logical engine; the logical engine examines the results of the tests and a security policy to determine whether to allow or block the Downloadable. See col. 6, lines 49-67. Hence, in view of the invention of Touboul '194, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Jerger such that the object is one of a COM object or an ActiveX control. One would be motivated to do to provide a fine grained definition of security policy on any type of active content that is downloaded from the network. The aforementioned cover the limitations of claim 22.

Conclusion

40. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

41. Wallent et al. US 6,366,912 discloses a system and method of providing security in a browser against downloaded content by defining network security zones.

42. Touboul US 6,804,780, Touboul US 6,480,962, Touboul US 6,167,520 and Touboul et al. US 6,154,844 are related to cited reference Touboul US 6,092,194.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432